Department of
INFORMATION
TECHNOLOGY

Maryland Network Documentation and Access Policy

Last Updated: 01/31/2017

Contents

1.0 Purpose

Network documentation is critical to efficient troubleshooting, onboarding personnel, and recovery in the event of a data loss or an integrity-impacting event. Network documentation should be created and updated regularly to ensure accuracy. Additionally, the establishment of network access controls protects both the network and data when a policy is not met by a user or device. The Maryland Department of Information Technology (DoIT) is responsible for, and committed to, managing the confidentiality, integrity, and availability of State government information technology (IT) networks, systems, and applications within the scope of its authority. This includes ensuring that networks are properly documented, configured, and accessed by Maryland agencies and users.

This policy mandates the creation of network documentation and network access-control standards for the DoIT Enterprise Network and all other agency networks under the policy authority of DoIT. The Maryland Department of Information Technology (DoIT) will utilize baseline controls and standards established by NIST SP 800-53R4 to direct this policy.

2.0 Document and Review History

This policy supersedes the Maryland Information Security Policy v3.1 (2013) Section 3: Asset Management and any related policy regarding network architecture and documentation declared prior to the 2017 Cybersecurity Program Policy. This document will be reviewed annually and is subject to revision.

Date	Version	Policy Updates	Approved By:
01/31/2017	v1.0	Initial Publication	Maryland CISO

3.0 Applicability and Audience

This policy is applicable to all IT environments and assets utilized by any agency supported by, or under the policy authority of the Maryland Department of Information Technology. DoIT will be responsible for documenting the network architecture of the Enterprise ("Enterprise Architecture") in accordance with the requirements of this policy

Agencies under the policy authority, but not under direct management of DoIT, must independently comply with the requirements of this policy.

4.0 Policy

This policy outlines the level of network documentation required by agencies, who has access to network documentation, and how changes to the network environment must be handled and communicated to stakeholders. Furthermore, this policy establishes the requirement to implement network access controls through device and user authentication to maintain the security posture of a network.

4.1 Network Component Documentation

Agencies must maintain an inventory of their network components in an asset-management repository in accordance with the *Asset Management Policy*. Asset inventory and network device documentation will follow the requirements outlined below.

#	Name	Requirement
A	Asset Management and Configuration Baseline	Network structure and configuration shall be documented and maintained through an Asset Management application, where possible, and shall document the following network components: ▪ Servers — Including the data on each server and location and schedule of backups ▪ Routers ▪ Switches ▪ Firewalls ▪ Hubs At minimum, configuration details shall include: ▪ IP address ▪ Protocol ▪ Default gateway ▪ Physical Location ▪ Logical Location ▪ OS version ▪ Patch Status NOTE: See *Configuration Management Policy* and *Asset Management Policy* for further details.
B	Non-Enterprise Agency Requirements	Agencies under the policy authority, but not managed by DoIT must exercise due care and due diligence to maintain updated network documentation.
C	Enterprise Requirements	Agencies under the IT management of DoIT must assist DoIT in maintaining up-to-date documentation.
D	Confidentiality of Network Documentation	All network documentation is considered confidential information, and will only be released to agency cybersecurity and IT management employees. ▪ Network documentation may be released to other personnel on a need-to-know basis NOTE: Help Desk and Security Operations Center (SOC) personnel will have read access to network documentation. ▪ These restrictions apply to network documentation in any form, whether written reports or topology diagrams

Network Topology Diagram Requirements

Agencies must create a network topology diagram that identifies the major network nodes and interconnections and meets the requirements outlined below.

#	Name	Requirement
E	Automatic Mapping	Network topology diagrams may be created using automatic tools used for **network mapping**. Assets discovered by network mapping must be: ▪ Physically verified and logically correlated ▪ Compared to other manually created documentation
F	Network Design Information	Diagram must include both physical and logical network design.
G	Information to Diagram	Diagram must, at minimum, depict: ▪ Routers ▪ Servers ▪ Gateways ▪ Other major pieces of networking hardware
H	Interconnections	Diagram must show the interrelationship between all network devices with lines indicating directional relationship.
I	Segment Maps	Diagram must include all segments of a network. ▪ Larger networks can have a general network map, with more specific maps for each individual segment, e.g., a general Enterprise Architecture map, with more specific maps for details of the Shared Services Block (SSB), Hosting Services Block (HSB), and each agency enclave ▪ Agencies that have isolated and segmented network structure due to confidential information must document all segments
J	Changes to Diagrams	Changes on the network must be documented on the topology diagrams within 30 days of the change to ensure that network topology diagrams stay up to date.
K	Storage and Access to Diagrams	Network topology diagrams are considered confidential information, and will only be released to agency cybersecurity and IT management employees. ▪ Network diagrams may be released to other personnel on a need-to-know basis NOTE: Help Desk and Security Operations Center (SOC) personnel will have read access to network topology diagrams ▪ Contractors or vendors who require access to the diagrams for the purposes of carrying out a project or task will be given authority to *access* or *view* topology diagrams. ▪ Contractors will only be given *editing* privileges, if explicitly authorized by the relevant personnel below: ◆ State CISO or delegated authority (Enterprise) ◆ Deputy CIO or delegated authority (for agencies not actively managed by DoIT)

4.2 Network Access Control

Agencies must restrict access to their network infrastructure only to trusted endpoints (e.g., those devices known to the network or configured to a secure baseline). Endpoint access-control enforces security by ensuring that endpoints or users meet security requirements prior to accessing the network.

#	Name	Requirement
A	**Network Access Control (NAC)**	Agencies must use Network Access Control to restrict availability of network resources to those endpoints that comply with a defined security baseline. ▪ New devices that connect to the network must not be permitted to access network resources until the system is fully compliant with the established security baseline ▪ Automatic NAC solutions, such as **802.1X** should be implemented, where possible ▪ NAC solutions must allow network administrators to define rulesets and access-rights based on documented use cases (see section 4.2(B))
B	Documentation of Security Baselines (Standard)	Agencies must establish and document standard security baselines for NAC.
C	Documentation of **Use Cases**	Use case scenarios must be created that outline various personnel categories and respective access control requirements for each category (e.g., State employee using a State issued device as opposed to a State contractor using a non-State issued device).
D	User Authentication	Network Access Control solutions must be able to authenticate down to the user-level granularity.
E	Device Authentication	Network Access Control solutions must be able to authenticate at the machine or device-level (i.e., MAC level).
F	**Roles Based Access Control (RBAC)**	Administrators must grant access rights based on specific role or function.
G	Segmentation	Network infrastructure must be segregated into distinct segments according to security requirements and service functions.
H	Least Privilege	▪ Users or guests should be granted access only to those resources that they need and only for the period of time necessary to fulfill their job related duties. ▪ Users or guests authorized to access a segment of a network must not be able to automatically access other isolated segments unless specifically authorized to do so.

4.3 Change Control

Changes applied to network devices (including boundary control devices) must be approved in accordance with the *Configuration Management Policy*. This ensures that all changes are properly reviewed for risk, security, and functionality through a Change Control Board before implementation on the network. Configuration management processes must be followed regardless of whether or not the change is a temporary or a permanent configuration change and must meet the requirements below.

#	Name	Requirement
A	Change Control	Change and configuration changes to network components must adhere to the DoIT *Configuration Management Policy* and associated configuration management processes.
B	Communication of Changes	▪ Changes or configurations to network components must be communicated to stakeholders Help Desk, SOC staff, server administrators, and IT

#	Name	Requirement
		Management personnel as soon as possible after network changes are made; these stakeholders could be notified by the change management process ▪ A spreadsheet or logging file will list all approved change requests or low risk changes, contain a detailed summary of action items, and be available by the above personnel for reference at any time
C	Examples of Configuration Changes	The following is a non-exhaustive list of configuration changes requiring notification: ▪ Reboot of a network device or loss of service or system availability ▪ Change of rules or configuration of a network device ▪ Upgrade to any software on a network device ▪ Installation and removal of any software on a network device ▪ Significant patch updates or major revision upgrades to authorized software ▪ New type of traffic allowed through a boundary device ◆ New protocols and services ◆ Application of a current rule to information systems of a higher security categorization than the rule currently applies to (as this may degrade or jeopardize the security of the higher-category device)

5.0 Exemptions

This policy is established for use within the DoIT Enterprise. If an exemption from this policy is required, an agency needs to submit a DoIT Policy Exemption Form and clearly articulate the reason for the exemption. An operational risk assessment will be conducted to identify the risks and the agency's mitigation strategy associated with this exemption. If the agency can accept the risk, an exemption to this policy may be granted.

6.0 Policy Mandate and References

The Cybersecurity Program Policy mandates this policy. Related policies include:

- Asset Management Policy
- Boundary Protection and Internet Access Policy
- Configuration Management Policy

7.0 Definitions

Term	Definition
802.1x	A networking protocol that provides an authentication mechanism to devices wishing to attach to a LAN or WLAN
Network Access Control (NAC)	A feature provided by some firewalls that allows access based on a user's credentials and the results of health checks performed on the telework client device
Network Mapping	A graphical representation of all the computers and devices on your network that shows how each is connected; this may be done by software that discovers devices on the network and their respective connectivity

Term	Definition
Role Based Access Control (RBAC)	A model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities
Use Cases	A list of actions or steps defining the interaction between a role and a system

8.0 Enforcement

The Maryland Department of Information Technology is responsible for enforcing policies for Enterprise onboarded agencies. The DoIT Cybersecurity Program identifies the minimum requirements necessary to comply with the information security standards and guidelines provided within Cyber Security Program Policy and its supporting policies. Agencies under the policy authority, but not under direct management of DoIT, must exercise due diligence and due care to independently comply with the minimum requirements of this policy or complete a Policy Exemption Request Form.

If DoIT determines that an agency is not compliant with this policy or any supporting policy, the non-compliant agency will be given a sixty (60) day notice to become compliant or at least provide DoIT a detailed plan to meet compliance within a reasonable time before the issue is reported to the Secretary of Information Technology. After which, the Secretary of Information Technology, or a designated authority, may extend a non-compliant agency's window of resolution or authorize a DoIT representative to limit or restrict an agency's access to external and internal communications (effectively shutting down connectivity) until such time the agency becomes compliant.